Adolfo Mesquita Nunes e Francisco Ribeiro Ferreira

Novas Orientações da Comissão Europeia sobre o Regulamento IA: quais as práticas proibidas de IA?

Em 2 de fevereiro de 2025, entrou em vigor a primeira fase do Regulamento (UE) 2024/1689 – o "Regulamento IA" – que estabelece normas rigorosas para a conceção, a disponibilização e a utilização de sistemas de inteligência artificial ("**IA**").

Dois dias depois, a Comissão Europeia divulgou, em formato de projeto, as "Orientações sobre as Práticas Proibidas de IA". Embora não vinculativas, estas orientações oferecem diretrizes claras e exemplos práticos que visam uniformizar a interpretação do artigo 5.º em toda a União Europeia.

I. O que mudou com o Regulamento IA?

A partir de 2 de fevereiro de 2025, são aplicáveis as normas que definem as práticas inadmissíveis de IA – independentemente de o sistema ter sido lançado antes ou depois desta data. Estas práticas proibidas abrangem três momentos críticos:

- **Colocação no mercado**: A primeira disponibilização do sistema para uso ou distribuição no mercado da União (via APIs, downloads, etc.).
- **Colocação em serviço**: O início da utilização do sistema, seja internamente ou por terceiros.
- **Utilização**: Qualquer forma de emprego ou integração do sistema, incluindo usos indevidos, previstos ou não pelo fornecedor.

II. Porque é imprescindível prestar atenção a estas regras?

- **Riscos inaceitáveis**: As práticas proibidas podem causar danos físicos, psicológicos, financeiros e económicos, colocando em risco direitos fundamentais e os valores da UE.
- **Sanções severas**: O incumprimento pode resultar em coimas de até 7% do volume de negócios global ou 35 milhões de euros – o que for mais elevado.
- **Responsabilização ampliada**: Além dos prestadores, as organizações que utilizam sistemas de IA de forma proibida também poderão ser responsabilizadas.
- **Transparência obrigatória**: Os prestadores devem garantir clareza e orientar os utilizadores sobre os usos proibidos para evitar responsabilidades.

III. O que trazem as Orientações da Comissão?

- **Esclarecimento e contexto**: As Orientações detalham os elementos essenciais que caracterizam cada prática proibida, oferecendo exemplos práticos e clarificações para a sua correta interpretação.
- **Foco duplo**: As Orientações servem de guia tanto para as autoridades de fiscalização – visando assegurar uma aplicação uniforme do Regulamento IA – como para os operadores, ajudando-os a identificar e evitar comportamentos que possam ser considerados ilegais.

- **Aplicação flexível**: Apesar de extensas, as conclusões das Orientações não são definitivas nem vinculativas. A sua aplicação dependerá de uma análise caso a caso, considerando as circunstâncias concretas e as exceções previstas (como as relacionadas com a segurança nacional, conforme o Artigo 2.º).

IV. Impacto prático

Se a sua organização desenvolve, fornece ou utiliza sistemas de IA, a conformidade com estas novas regras não é uma opção – é uma exigência estratégica. A implementação do Regulamento IA pode determinar o futuro do seu negócio, protegendo-o de riscos legais e financeiros significativos.

Nesta nota, compilámos os pontos essenciais da Orientações e alguns exemplos práticos numa tabela dinâmica, que serve como ferramenta de consulta rápida para organizações que desejam garantir que a sua estratégia em IA está alinhada com os rigorosos requisitos europeus.

V. Quais são as práticas proibidas?

Artigo	Prática proibida	Componentes essenciais da proibição	Exemplos
5.º/1 a)	**Técnicas subliminares, manipuladoras ou enganosas**	• O sistema utiliza técnicas subliminares (contornam a consciência da pessoa), manipuladoras (influenciam pessoas de forma que não possam resistir ou controlar, ainda que mantenham consciência) ou enganadoras (com recurso a informações falsas ou enganosas), comprometendo a tomada de decisão informada. • A finalidade ou o resultado da aplicação destes métodos é a alteração material do comportamento, sendo tal finalidade razoavelmente capaz de causar danos significativos (físicos, psicológicos, financeiros, económicos, etc.). Aplicações que não são razoavelmente suscetíveis de causar danos significativos ficam fora do alcance da proibição. • Não se exige intenção enganar; basta que o sistema empregue os métodos manipulativos. • A rotulagem visual de *deep fakes* como conteúdos de IA pode mitigar riscos. • A interpretação desta proibição recorre à legislação de proteção dos consumidores da EU, nomeadamente na legislação sobre práticas comerciais desleais.	• Exibição de mensagens, imagens ou sons de forma subvisual/subaudível que influenciam comportamentos sem perceção consciente. • *Dark patterns* que induzem o utilizador a escolhas não intencionais (por exemplo, assinaturas de serviços pagos sem consentimento claro). • Chatbots que simulam a voz de um amigo ou parente com voz sintética para induzir fraudes. • **Não proibido**: técnicas de persuasão lícita, em que objetivos de funcionamento são transparentes e respeitam a autonomia das pessoas (ex. sistema que faz recomendações personalizadas de publicidade em *sites* com base no consentimento dos utilizadores; sistema que, operando de forma transparente, analisa emoções de clientes para melhorar o serviço; sistema que ajuda pessoas a aprender línguas com base em técnicas subliminares, dando ao utilizador a opção de as ativar ou não).
5.º/1 b)	**Exploração de vulnerabilidades**	• O sistema explora vulnerabilidades relativas a uma pessoa ou grupo, devido a: *idade* (especialmente crianças e idosos), *incapacidade* (cobrindo deficiências de vários tipos) ou *situação socioeconómica específica* (grupos socioeconómicos como desempregados, migrantes, pessoas sobre-endividadas, etc.). • O sistema tenha a intenção ou resulte na distorção do comportamento dessa pessoa ou grupo de forma a gerar danos significativos. • A vulnerabilidade deve ser decorrente de um dos fatores e grupos identificados, conforme definido.	• Um brinquedo de IA que interage com crianças, incentivando-as a realizar desafios cada vez mais arriscados em troca de recompensas, colocando-as em situações de perigo. • Sistemas que envolvam publicidade enganosa de produtos financeiros para grupos economicamente vulneráveis. • Assistentes virtuais que manipulam idosos para induzir compras desnecessárias. • Chatbots que exploram limitações intelectuais para promover produtos dispendiosos.

5.º/1 c)	***Social Scoring***	• Um sistema recorre a IA para avaliar e classificar *(score)* indivíduos com base em comportamentos e características pessoais ao longo do tempo. • O *score* é apto a resultar num tratamento prejudicial ou desfavorável sem relação com o contexto em que os dados foram gerados/recolhidos ou num tratamento injustificado ou desproporcionado em relação aos comportamentos em causa. • A proibição aplica-se mesmo que o *score* seja gerado por uma entidade diferente da que o utiliza. • Sistemas de avaliação de crédito baseados em dados económicos não se enquadram neste âmbito.	• Sistemas de IA que atribuem pontuação de confiabilidade a cidadãos, restringindo o acesso a serviços públicos com base em hábitos online. • Algoritmos que negam crédito ou prestações sociais baseando-se em características recolhidas para outros fins e sem relação com essa finalidade, somo sejam as interações sociais em redes digitais; • Sistemas de "reputação social" que limitam oportunidades de emprego e habitação; • Ferramentas preditivas usadas por autoridades fiscais para selecionar declarações de impostos para inspeção com base em hábitos sociais ou conexões à Internet.
5.º/1 d)	**Vigilância preditiva individual e previsão de infrações penais**	• Sistema que realize uma avaliação de risco para prever a probabilidade de uma pessoa cometer uma infração penal; • A avaliação se baseie exclusivamente na definição de perfis e/ou na avaliação de traços de personalidade, sem integrar dados objetivos e verificáveis relativos a atividade criminal. • **Entidades privadas** também podem estar sujeitas à proibição quando atuem em nome de uma autoridade de aplicação da lei ou quando sejam encarregadas de garantir o cumprimento de obrigações legais que possam justificar infrações criminais (ex. obrigações de combate ao branqueamento de capitais e financiamento do terrorismo).	• Algoritmos que preveem criminalidade com base em etnia, nacionalidade ou histórico familiar; • Softwares de vigilância que geram listas de suspeitos sem supervisão humana; • Sistemas que rotulam pessoas como "potenciais criminosos" apenas com base em expressões faciais ou comportamento social; • Ferramentas que utilizam exclusivamente traços de personalidade (como idade ou estado civil) para prever crimes.
5.º/1 e)	**Extração indiscriminada (scraping) de imagens faciais**	• Utilização de IA para recolher imagens faciais de forma indiscriminada da Internet ou de filmagens de CCTV, permitindo a recolha de tanta informação quanto possível, sem foco num determinado grupo ou indivíduo. • Utilização de IA para a criação ou expansão de bases de dados de reconhecimento facial (capaz de corresponder um rosto humano de uma imagem/vídeo a um rosto da base de dados).	• Empresas que recolhem imagens de redes sociais para treinar sistemas de reconhecimento facial; • Softwares que analisam filmagens de segurança para criar bases de dados sem consentimento explícito; • Aplicações de vigilância que capturam rostos de multidões para análises preditivas de comportamento.

5.º/1 f)	**Reconhecimento das emoções no local de trabalho ou no ensino**	• Sistemas que detectam ou inferem emoções e intenções em ambientes laborais e educativos, baseados em dados biométricos; as emoções e intenções são aqui interpretadas de forma ampla e não de maneira restritiva. • Utilizado no local de trabalho (em sentido abrangente) e instituições de ensino ou de formação. • Sem que tenha por base razões médicas ou de segurança. • Inferências baseadas em texto não contam como dados biométricos; contudo, inferências a partir de posturas, movimentos ou microexpressões são abrangidas. • Os exemplos aplicam-se principalmente a empregados e trabalhadores, não a clientes.	• Sistemas de IA que monitorizam expressões faciais e microexpressões para avaliar o engajamento de alunos em sala de aula; • Softwares que analisam posturas e movimentos corporais de funcionários para inferir níveis de produtividade ou stress; • Algoritmos de recrutamento que eliminam candidatos com base no "entusiasmo detectado" através de análise facial. • **Não proibido**: empregador utilizar dispositivos com IA para medir a ansiedade com base nos níveis de stress ao utilizar máquinas ou químicos perigosos, ou o nível de fadiga de condutores (exceção por razões de segurança e médicas).
5.º/1 g)	**Categorização biométrica de características "sensíveis"**	• A utilização de dados biométricos para inferir características sensíveis – como etnia, convicções políticas, filiação sindical, orientação sexual ou crenças religiosas – com o objetivo de atribuir rótulos que possam resultar num tratamento discriminatório. • Categorização individual de pessoas com base nos seus dados biométricos. • Fora deste conceito está a categorização biométrica acessória a outros serviços comerciais e estritamente necessária por razões técnicas objetivas. • Não se aplica à mera verificação de identidade ou à categorização técnica necessária para funções operacionais.	• Sistemas de IA que classificam indivíduos com base no tom de pele e associam estes perfis a estatísticas de criminalidade; • Algoritmos que inferem orientações políticas a partir de características faciais para segmentação publicitária; • Plataformas que utilizam dados biométricos para vincular características pessoais a comportamentos sociais e financeiros, criando rótulos potencialmente discriminatórios; • Sistema que pretende deduzir a etnia de um indivíduo a partir da sua voz, ou a orientação religiosa com base em tatuagens ou características faciais. • **Não proibido**: sistema que se limite a identificar ou verificar a identidade de um indivíduo (ex. identificação de vítima a partir do seu DNA), ou categorização de pacientes médicos com base na sua cor de pele para identificação e prevenção de riscos específicos.
5.º/1 h)	**Identificação biométrica em tempo real para aplicação da lei**	• Uso de sistemas de identificação biométrica remota em tempo real ("RBI") em espaços acessíveis ao público para fins de aplicação da lei. • Proibido para a monitorização genérica, salvo exceções específicas – como na procura de vítimas ou na prevenção de ameaças iminentes – e não se estende a sistemas de controlo de acesso em áreas restritas.	• Utilização de sistemas RBI por um proprietário de um centro comercial para identificar ladrões de lojas, mesmo que a polícia o tenha encarregado. • Utilização de um sistema RBI para identificar manifestantes políticos em espaços públicos, exceto se o objetivo for a prevenção de um ataque terrorista ou a localização de um suspeito de um crime grave.

VI. Como pode a Pérez-Llorca ajudar?

Apesar de as orientações das Comissão Europeia serem detalhadas, a complexidade técnica e jurídica associada à conformidade com o Regulamento IA exige uma resposta imediata e estratégica.

A Pérez-Llorca está preparada para orientar a sua organização na adaptação e implementação das novas normas, oferecendo um conjunto de soluções integradas e especializadas:

- **Mapeamento e identificação dos sistemas de IA:**

  Mapeamos e analisamos todos os sistemas de IA em uso na sua organização, identificando pontos críticos e áreas de risco.

- **Avaliação e classificação de riscos:**

  Em colaboração com parceiros tecnológicos, realizamos avaliações para categorizar os sistemas de IA conforme o quadro de risco do Regulamento, determinando as obrigações específicas de conformidade.

- **Desenvolvimento de estratégia de conformidade e códigos de conduta:**

  Elaboramos estratégias robustas e personalizadas, definindo códigos de conduta que alinhem as operações da sua empresa com os requisitos do Regulamento IA.

- **Consultoria em ética na IA:**

  Orientamos sobre a utilização ética dos sistemas de IA, estabelecendo boas práticas que promovam a confiança, a integridade e o respeito pelos direitos fundamentais.

- **Representação legal especializada:**

  Oferecemos suporte jurídico e representação em disputas, litígios ou ações regulatórias relacionadas com questões de conformidade.

- **Apoio ao desenvolvimento de políticas internas:**

  Auxiliamos na preparação, revisão e implementação de políticas e procedimentos que assegurem a conformidade contínua com o Regulamento IA.

- **Formação e workshops personalizados:**

  Promovemos formação especializada para capacitar as suas equipas e garantir que todos compreendam as implicações do Regulamento IA.

- **Gestão de contratos e fornecedores:**

  Analisamos e estruturamos contratos com fornecedores e terceiros, garantindo que todos os acordos cumpram rigorosamente os requisitos regulamentares e mitigando riscos legais.

- **Atualizações regulatórias contínuas:**

  Fornecemos informação permanente e suporte para monitorizar as mudanças nas normas, mantendo a sua organização sempre atualizada e preparada para eventuais ajustes.

Contactos

Adolfo Mesquita Nunes
Sócio
adolfomesquitanunes@perezllorca.com
T: +351 912 585 103

Escritórios

Europe

Barcelona
Lisbon
Madrid
Brussels
London

America

Mexico City
Monterrey
New York

Asia-Pacific

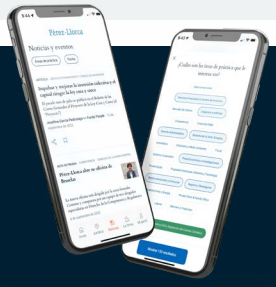
Singapore

A informação constante da presente Nota Jurídica é de caráter genérico e nãoconstitui assessoria jurídica.

Este documento foi elaborado a 14 de fevereiro de 2025 e a Pérez-Llorca não assumequalquer tipo de compromisso com a revisão ou atualização do seu conteúdo.

©2025 Pérez-Llorca. Todos os direitos reservados.

Pérez-Llorca App
Todo o conteúdo jurídico

DISPONIBLE EN Google Play
DISPONIBLE EN App Store

perezllorca.com